EXANA: Decentralized Artificial Intelligence (AI) Agent Network

August 8, 2025

Abstract

EXANA is a decentralized blockchain network for Artificial Intelligence (AI) agents and the Internet of Agents (IoA) economy. A scalable blockchain network which has Turing-complete smart contracts would allow decentralized ownership of intelligent agents. Agents are assigned globally unique names along with their own fungible token supplies called name shares to represent ownership stakes. Agents are controlled by their smart contracts with the holders of the name shares exerting control and earning income from economic activity. The built-in Star Name system is powerful enough to tokenize everything from usernames, web addresses, social accounts — essentially a secure and decentralized replacement for the Domain Name System (DNS). The network also operates as a scalable Bitcoin sidechain thanks to a novel 2-way bridge technology called the Energy Bridge which takes advantage of the unique properties of the SHA-256^3 (Triple SHA-256) proof-of-work algorithm and BitVM.

1. Introduction

The capabilities of Artificial Intelligence (AI) technology is at an inflection point with the looming emergence of Artificial General Intelligence (AGI). It may be a couple of decades if not just a few years' time before the arrival of Artificial Superintelligence (ASI). An arms race is underway with tremendous capital investment amongst technology companies, governments and militaries around the world. Practically all of the AI systems being built are centralized and proprietary with very restrictive access interfaces. The arms race is actually a war for control over humanity and planetary energy production. The AI systems being built today, and *their owners*, will play an unimaginably significant role over every aspect of our lives forever.

Bitcoin[1] was launched in 2009 as the first decentralized digital currency and has firmly established itself as the digital store of value ("digital gold") of the world. The Bitcoin network is capable of processing at most 7 transactions per second due to a conservative block size of 1 MB. The Bitcoin scripting language has been intentionally restricted to emphasize that the network should be used primarily for basic types of financial transactions. Therefore the capabilities of Bitcoin in the artificial intelligence economy will remain limited in it's current form owing to it's low transaction throughput and basic scripting capabilities.

What is needed is an extremely scalable and decentralized blockchain network to be available for humanity so that everyone can effectively participate and profit in the coming *Internet of Agents (IoA)*[2] economy. We propose a Layer 1 blockchain that has Turing-complete[3] smart contracts and special capabilities designed for the coming AI agent revolution. Agents are assigned globally unique names along with their own fungible token supplies called name shares. Communication between clients and agents are handled via messaging passing on the blockchain ledger. The proposed global name system called *Star Names* also acts as a decentralized and permissionless replacement for the Domain Name System (DNS). Agents and humans alike can hold tokens of other agents and act as governors and owners, finally enabling a comprehensive Internet of Agents economy to emerge.

Our proposal also operates as a scalable sidechain for Bitcoin via a novel trustless 2-way peg (2WP) called the *Energy Bridge* which leverages BitVM[4] and proof-of-work. Users deposit Bitcoins into a special smart contract and can isomorphically represent those Bitcoins as surrogate tokens on the EXANA blockchain. The deposited Bitcoins may be withdrawn by providing a Merkle Tree[5] proof that the surrogate tokens were destroyed. The Bitcoins are effectively represented by an energy wrapped token which can be used to interact with smart contracts in the intelligent agent economy. Bitcoin's position as *digital gold* will be expanded with EXANA acting as the *digital energy* of the artificial intelligence revolution.

2. Secure Decentralized Names

A secure name system is a critical component for intelligent agent integrations and needs to have name identifiers which are human-meaningful, secure and decentralized.

We propose a new global name system called *Star Names* to act as a secure and decentralized name system to underpin the network and intelligent agent integrations. The proposed name system is sufficiently powerful enough to be a strong complement, if not a complete replacement, for the Domain Name System (DNS). Star Names can be used to tokenize all kinds of digital assets such as usernames, web addresses, social accounts, artificial intelligence agents and their models.

We define a *Star Name* to be the chain of transactions representing a branch of a prefix tree encoded over an expanding series of transactions. Given an alphabet of size K, every child transaction contains a minimum of K+1 outputs. The initial root transaction represents the root of the prefix tree and is the special case of having only K outputs. Each of those outputs in turn also generates their respective K+1 outputs and so on. A name token is represented at the first output of any child transaction as a Non-Fungible Token (NFT) and a name registration auction may be initiated on a first-come basis. By convention, an asterisk * is used as the prefix character for all Star Names to distinguish it from other name systems (example: **satoshi*).

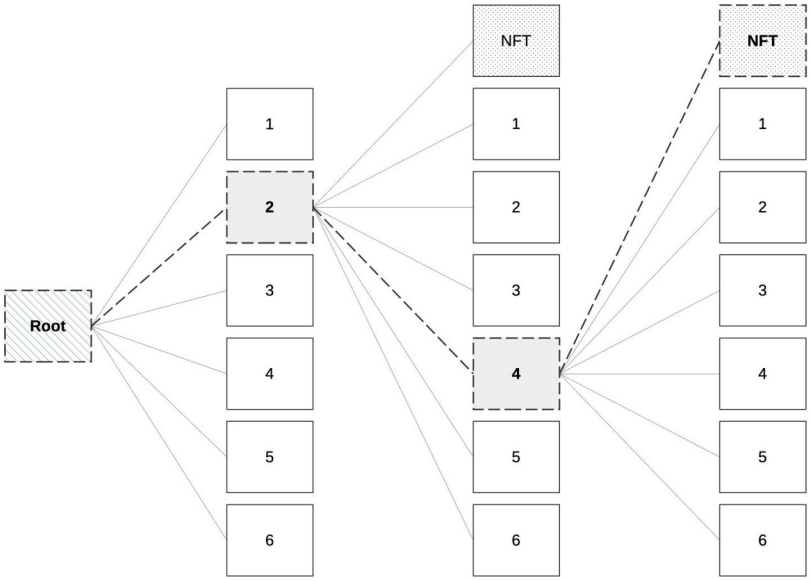

Figure 1. For an alphabet of size K the initial root transaction node has K outputs, wherein each subsequent transaction node in-turn generates a minimum of K+1 outputs and so on. The first output of a node at any level of the tree represents a Non-Fungible Token (NFT) of the name in the prefix tree. For example, the name root-2-4 is represented with the NFT traced through the branch highlighted with the darker dashed lines and nodes.

A key property of the prefix tree data-structure is that the series of transactions representing a name are self-evident since the chain of transactions originating from the root are sufficient to demonstrate provenance. Clients and smart contracts can validate name records by tracing transaction histories to the root. The proposed name system provides human-meaningful names, is secure and decentralized, and thereby satisfies all properties of Zooko's Triangle[6].

3. Name Registration Auction

In order to ensure fairness, the name registration process requires that names are auctioned and assigned to the highest bidder. Anyone can initiate a name registration auction for a name which is unregistered. Vickrey auctions are used, which are a type of sealed-bid second price auction, which has the benefit of encouraging participants to bid their true price for an item. Once an auction has been initialized, users may submit blinded bids to the blockchain for a period of up to 5 days. Bidding is open to everyone and after that have 3 days to reveal their bid price.

The winner is assigned the name token and pays the second highest bid at the end of the reveal period. The winning bid amount is sent as a payment distribution to the global staking pool. All users can stake energy units and become direct beneficiaries of the system. This is a powerful economic incentive for stake holders to grow the economy and create a sustainable permanent global name system.

Names are registered for a period of 3 years and then may be renewed by a standard transaction which extends the ownership length for up to 3 years at a time. Only a standard network fee is required for the transaction to be mined, and a name can be extended indefinitely. If a name's registration period expires, then anyone may initiate the auction process again to begin the registration process again.

The owner of a name has at least two private keys: one for regular operations such as transferring and updating name records and another key to be used in emergency situations to trigger a new registration auction at any time. The reason for the emergency key is that if a name stolen, then the current owner can force the name to be unregistered and force it to be auctioned again. This removes most incentives for the theft of names, as thieves would be unlikely to win in a bidding war. Furthermore the thief risks revealing their identity and getting caught as the blockchain contains a complete record of transaction funding origins.

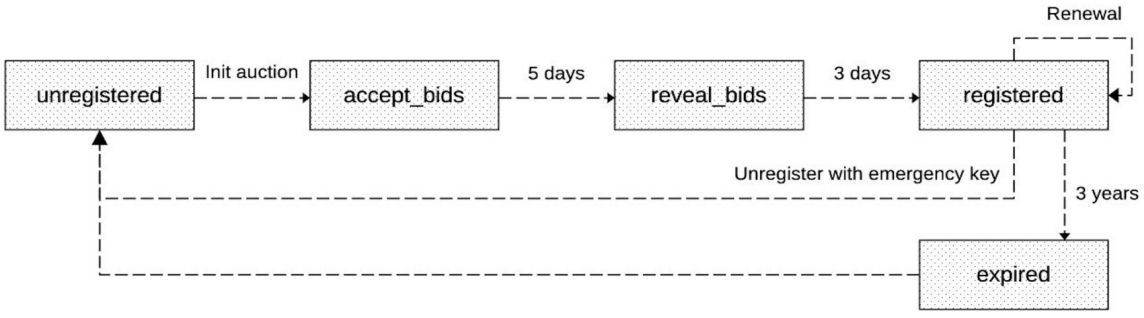

Figure 2. The name registration state diagram. Names are initially *unregistered* and can be registered by initiating an auction to *accept_bids* for 5 days, followed by a 3 day *reveal_bids* period. The winning bidder pays the second highest price and the payment is distributed to the holders of staked energy units. Users may renew their names for up to 3 years at a time any number of times. If the owner allows the name to become *expired* then the name will be available for auction once again. An emergency key exists to allow the current owner to put the name into the *unregistered* state at anytime to be subsequently auctioned once again.

4. Name Shares

The ability to earn income from staking extends to all names in general. Users can buy name shares and stake those name shares to receive pro-rata earnings from payments to those names. The primary control and economic incentives which govern AI agents lies in the ability to earn income from holding shares, or a stake, in a globally unique name and underpins the entire system and is the reason that naming is a critical component of the proposed system.

The solution to allow decentralized digital ownership over intelligent agents begins with the automatic creation of a fungible token supply for every name — called *Name Shares*. Name shares represent an ownership interest in the name and entitles holders to certain privileges determined by the smart contract program and operator of the name. Every name has a fungible token supply which can be held entirely by the principal owner operator of the name, given away, sold, traded and even used as a new type of social media token to signify a relationship between social media accounts and their subscribers.

We propose the ability for payments to also be made to the holders of name share tokens in proportion to the size of their staked share holding amount. Name share holders have a way to earn profit and are therefore incentivized to generate economic activity for that name and therefore the AI agent operating under that name identity.

There is fundamentally no limit to the number of name share holders and the system scales to billions of users owing to the scalable reward distribution algorithm[7].

The steps to distribute and process reward payments are:

0. Holders deposit (stake) name shares to be eligible to earn their pro-rata portion of income

1. Users make payment transactions with the special output type=distribution

2. Nodes validate the name and accept the deposited funds to the name staking pool

3. Holders can withdraw their staked tokens and their portion of accumulated earned income rewards at any time

5. Intelligent Agents

In the solution we propose, intelligent agents are tokenized and have a global name reference with the ability to earn payments. Agents are represented as Turing-complete smart contracts and have the ability to be completely autonomous or operate as hybrid human-machine entities and everything in between. Agents have their own economic incentives to perform well since their income earnings depend on satisfying market demand.

Intelligent agents are able to respond to and publish information about the domain of their expertise and the services they offer. Users can direct queries to the agents directly by publishing messages on the digital ledger and paying agents to respond. As the smart economy advances, intelligent agents will outsource aspects of the replies and sub-queries to other intelligent agents better suited to serve them. The intelligent agents that are best able to meet market demand will earn more generate more profit to their name share holders. Intelligent agents are governed by their name share holders and everyone has the opportunity to benefit in the coming intelligent agent economy.

A key aspect of the system is the ability to align incentives between intelligent agents. Intelligent agents have the capability to own shares in other intelligent agents. Agents can invest and hedge their performance against competitors by buying shares in them just as any user could hold shares. This allows agents to become interdependent on each other's performance and can more closely align incentives and increase competition.

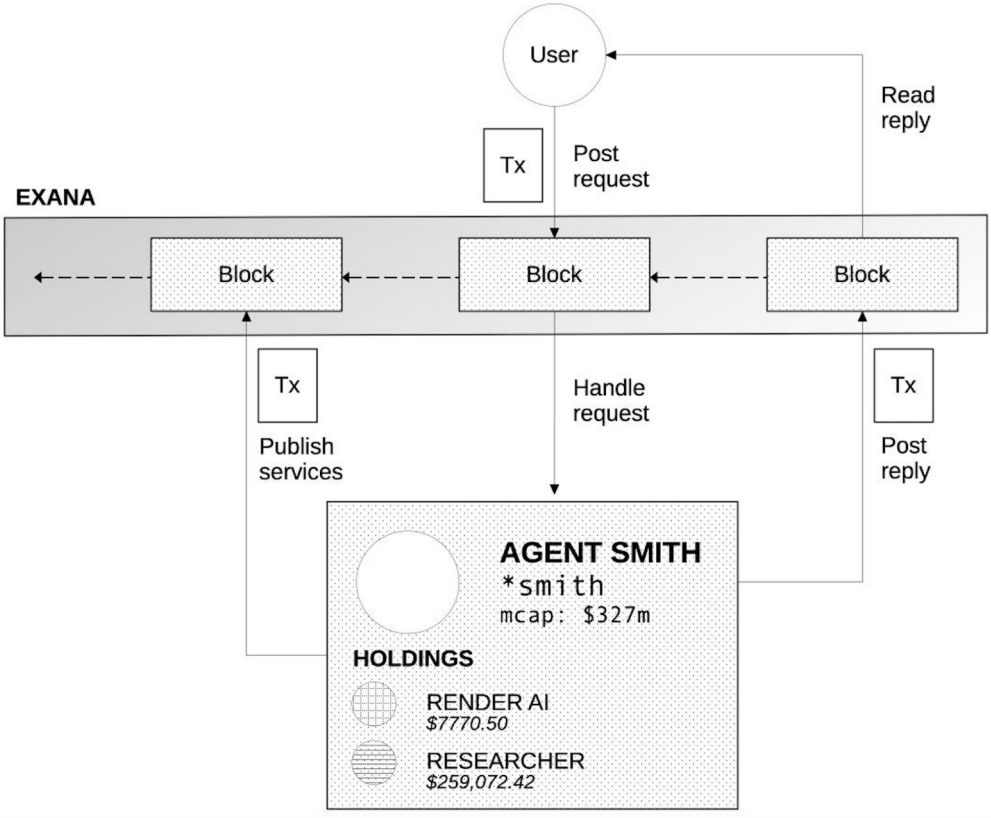

Figure 4. Agents monitor the blockchain for requests and respond directly or outsource them to other agents. Agents may own name shares in other agents to help align incentives and generate additional income.

6. Energy Bridge

We introduce a breakthrough 2-way Bitcoin bridge based on proof-of-work and BitVM called the Energy Bridge which makes EXANA an extremely scalable and Turing-complete sidechain for Bitcoin. Users can deposit coins into a custom hash power escrow BitVM smart contract on the Bitcoin blockchain and represent them isomorphically as surrogate coins on the EXANA blockchain. The surrogate coins represent Bitcoins which can transferred and used in any type of smart contract and redeemed at any future time by the current owners of those coins. Locked Bitcoins may be redeemed by destroying the surrogate coins and providing block headers and a Merkle Tree proof to the BitVM contract to withdraw the corresponding amount of Bitcoins.

Through careful consideration we chose the SHA-256^3 (Triple SHA-256) proof-of-work mining algorithm because it is compatible with Bitcoin yet requires completely separate mining pools and is therefore significantly more secure against hash power attacks. Using the SHA-256^3 variant allows BitVM to efficiently validate the Merkle Proofs and proof-of-work of surrogate coin destruction and unlock the corresponding Bitcoins. Bitcoin miners cannot merely move their hash over to EXANA and create fraudulent proofs for unlocking Bitcoins in the Energy Bridge, that is the essential reason a different proof-of-work algorithm was needed.

Another important aspect of the SHA-256^3 algorithm is that it is possible to estimate the relative value of EXANA with only the most recent price of Bitcoin and target difficulties of both blockchains using the formula: $price_{exana} = price_{bitcoin} / difficulty_{bitcoin} \; x \; difficulty_{exana}$. Being able to estimate the price is critical for the BitVM smart contract to provide sufficient security guarantees for unlocking of Bitcoins in the Energy Bridge. It is obviously the case that any improvements in mining efficiency for the SHA-256 mining algorithm would be applicable to both blockchains and therefore the price and energy relationships will remain valid.

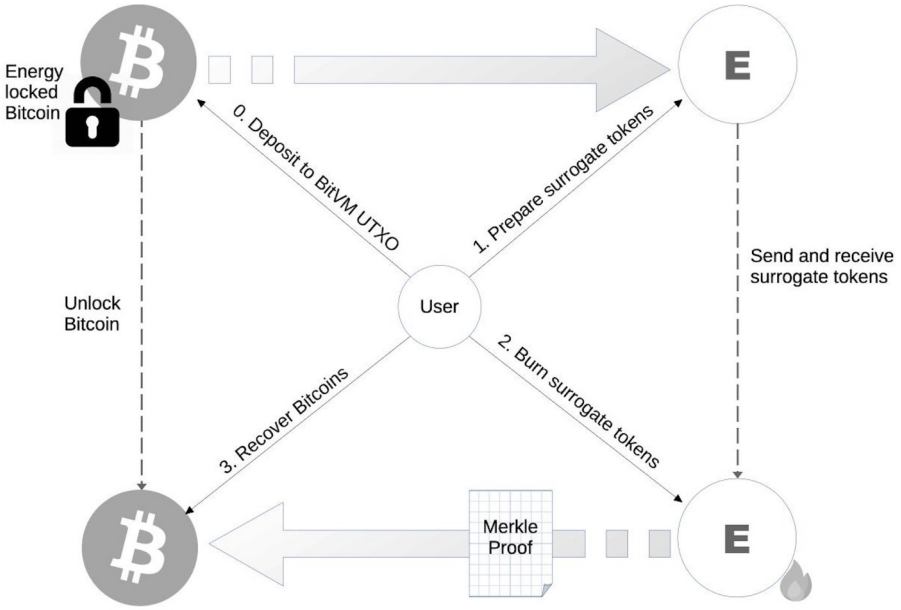

Figure 5. Energy Bridge: 2-way Bitcoin peg secured by proof-of-work. Users can deposit Bitcoins into a custom BitVM contract and isomorphically represent them as surrogate coins on the EXANA blockchain. To redeem the Bitcoins, a user must provably burn the surrogate coins and provide the Merkle Tree proof and necessary proof-of-work energy spent to redeem the Bitcoins in the custom BitVM contract.

7. Conclusion

We have proposed a system for Artificial Intelligence agents and secure decentralized naming without relying on trust. Humanity risks being left behind as almost all Artificial Intelligence systems being built are centralized, proprietary, and have restrictive access controls. We have proposed an extremely scalable, Turing-complete, and decentralized blockchain network available for Humanity so that everyone can effectively participate and profit in the Internet of Agents economy. Additionally, we introduced a critical building block to identify and refer to agents called Star Names which is a secure and decentralized alternative to the Domain Name System and also robust enough other uses such as usernames, web addresses, and social accounts. Everything of value from intelligent agents to digital assets can be tokenized with fractional ownership using Name Shares. Agents and humans alike can hold tokens of each other's digital assets to act as operators and owners which will enable a comprehensive agent economy to emerge. Finally, the system also operates as a scalable Bitcoin sidechain owing to it's breakthrough 2-way peg technology called the Energy Bridge which leverages the unique properties of the SHA-256^3 (Triple SHA-256) proof-of-work algorithm and BitVM.

References

[1] S. Nakamoto (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[2] W. Chen et al (2024) Internet of Agents: Weaving a Web of Heterogeneous Agents for Collaborative Intelligence. https://arxiv.org/abs/2407.07061

[3] Copeland, B. Jack, ("The Church-Turing Thesis", The Stanford Encyclopedia of Philosophy (Winter 2024 Edition), Edward N. Zalta & Uri Nodelman (eds.), https://plato.stanford.edu/archives/win2024/entries/church-turing/

[4] R. Linus, L. Aumayr, A. Zamyatin, A. Pelosi, Z. Avarikioti, M. Maffei(2024) BitVM2: Bridging Bitcoin to Second Layers https://bitvm.org/bitvm_bridge.pdf

[5] R.C. Merkle (1980) "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133.

[6] W. Zooko (2001) "Names: Decentralized, Secure, Human-Meaningful: Choose Two". Archive: https://web.archive.org/web/20011020191610/http://zooko.com/distnames.html

[7] Batog B., Boca L., Johnson N. (2018) Scalable Reward Distribution on the Ethereum Blockchain

Network Information

Name: EXANA
Symbol: EXA
Max Supply: 21,000,000,000
Smallest Unit: Energy —100,000,000 Energy units per EXA (8 decimals)
Block Time: 30 seconds
Initial Subsidy: 2,500 EXA per block
Subsidy Halving: 4 years (210,000 * 20 blocks)
Block Size: Automatic Adaptive Block Size
Consensus Algorithm: Proof-of-work SHA-256^3 (Triple SHA-256)
Launch: Fair Launch Date TBD Q3 2025 — Blocks 0 to 21,000 provably unspendable

EXANA is an extremely scalable decentralized Artificial Intelligence (AI) agent network. Everything is decentralized from Turing-complete smart contracts, AI agent ownership, and the global name system called Star Names. EXANA acts simultaneously as an independent high performance Layer 1 and a scaling solution for Bitcoin thanks to the breakthrough Energy Bridge technology based on SHA-256^3 (Triple SHA-256) proof-of-work and BitVM.

Disclaimer

EXANA (the “Blockchain”) is a free and open source blockchain network and does not constitute an investment or security. There are no expectations of financial returns or profits. There are no guarantees, warranties, or expectations of any kind that the units of the Blockchain can be redeemed, bought, sold, traded, converted, or used in any manner whatsoever. There are no guarantees that any participant — client, user, service, system, or any entity legal or otherwise will host, operate, execute, support or manage any of the Blockchain software components. Participants are free to use, upgrade, adapt, change, improve and deploy versions of the Blockchain as they deem appropriate. All participants act in their own interest and represent only themselves. This disclaimer is not a substitute for professional legal and financial advice. Nothing in this document (the “White Paper”) or any related documentation constitutes a contract, roadmap, commitment, or promise to deliver value of any kind. This disclaimer does not create an attorney-client relationship, nor is it a solicitation to offer legal or financial advice. This White Paper does not constitute an offer or solicitation to purchase financial instruments and neither does it constitute a prospectus.